

UbiComp – Teil 9: Industrial WLAN, Bluetooth & Zigbee

Prof. Dr.-Ing. Dorothea Schwung

Lernziele Teil 9

1. Sie können die Besonderheiten drahtloser Kommunikation benennen.
2. Sie kennen die Frequenzbereiche der drahtlosen Kommunikation.
3. Sie kennen die verschiedenen Dimensionen im Multiplexing und sind in der Lage diese näher zu erläutern.
4. Sie können die Unterschiede zwischen WLAN und Bluetooth erklären.
5. Sie verstehen das Konzept der Piconetze beim Bluetooth.
6. Sie wissen worauf Zigbee basiert und kennen die Anwendungsdomänen.

Industrial WLAN: Einsatzfelder drahtloser Kommunikation

Fahrerlose
Transportsysteme



Mobile Diagnose
Mobiler Service



Mobiles
Bedienen & Beobachten



Hochregallager



Roboter



Raue Umgebungen



Industrial WLAN: Vorteile drahtloser Kommunikation

- **räumlich flexibel** innerhalb eines Empfangsbereichs
- **Ad-hoc-Netzwerke** ohne vorherige Planung machbar
- **keine Verkabelungsprobleme**
- **unanfälliger gegenüber Katastrophen** wie Erdbeben, Feuer – und auch unachtsamen Benutzern, die Stecker ziehen!

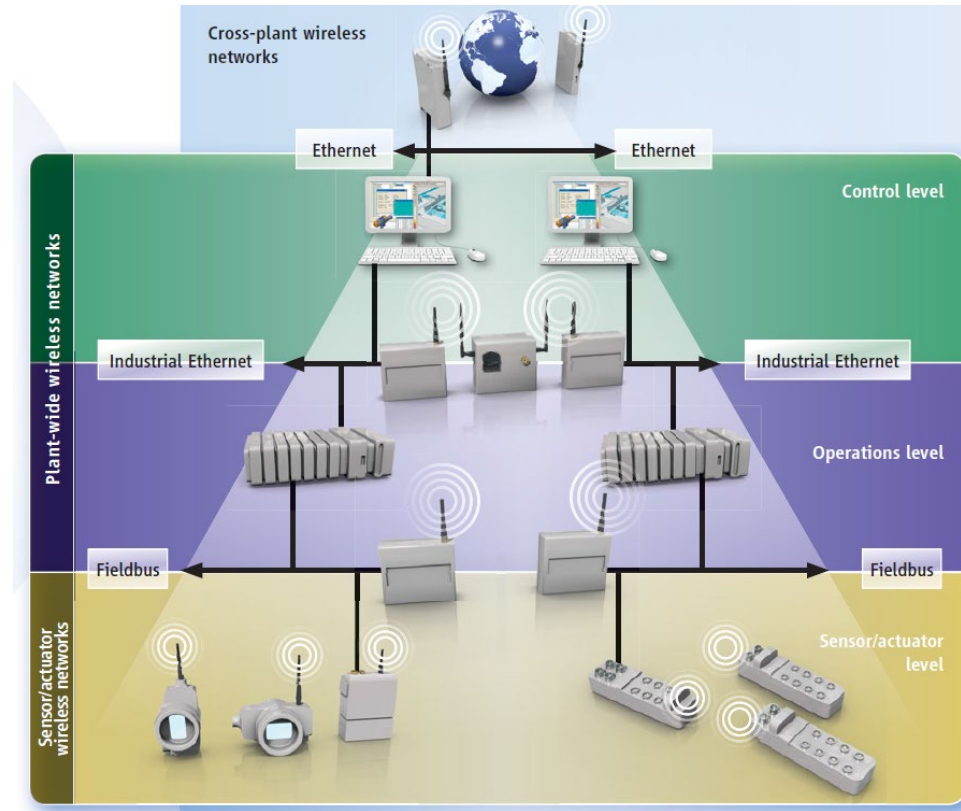
Industrial WLAN: Nachteile drahtloser Kommunikation

- im Allgemeinen sehr niedrige Übertragungsraten im Vergleich zu Festnetzen (1-10 Mbit/s) bei größerer Nutzerzahl
- Standards wie IEEE802.11 haben eine limitierte Performance
- teilweise proprietäre leistungsstärkere Lösungen
- Beim Arbeiten mit Funk sind viele nationale Restriktionen zu beachten, globale Regelungen werden erst langsam geschaffen (z.B. bietet Europa mehr Kanäle als die USA)
- Beschränkungen, was die Echtzeitfähigkeit angeht

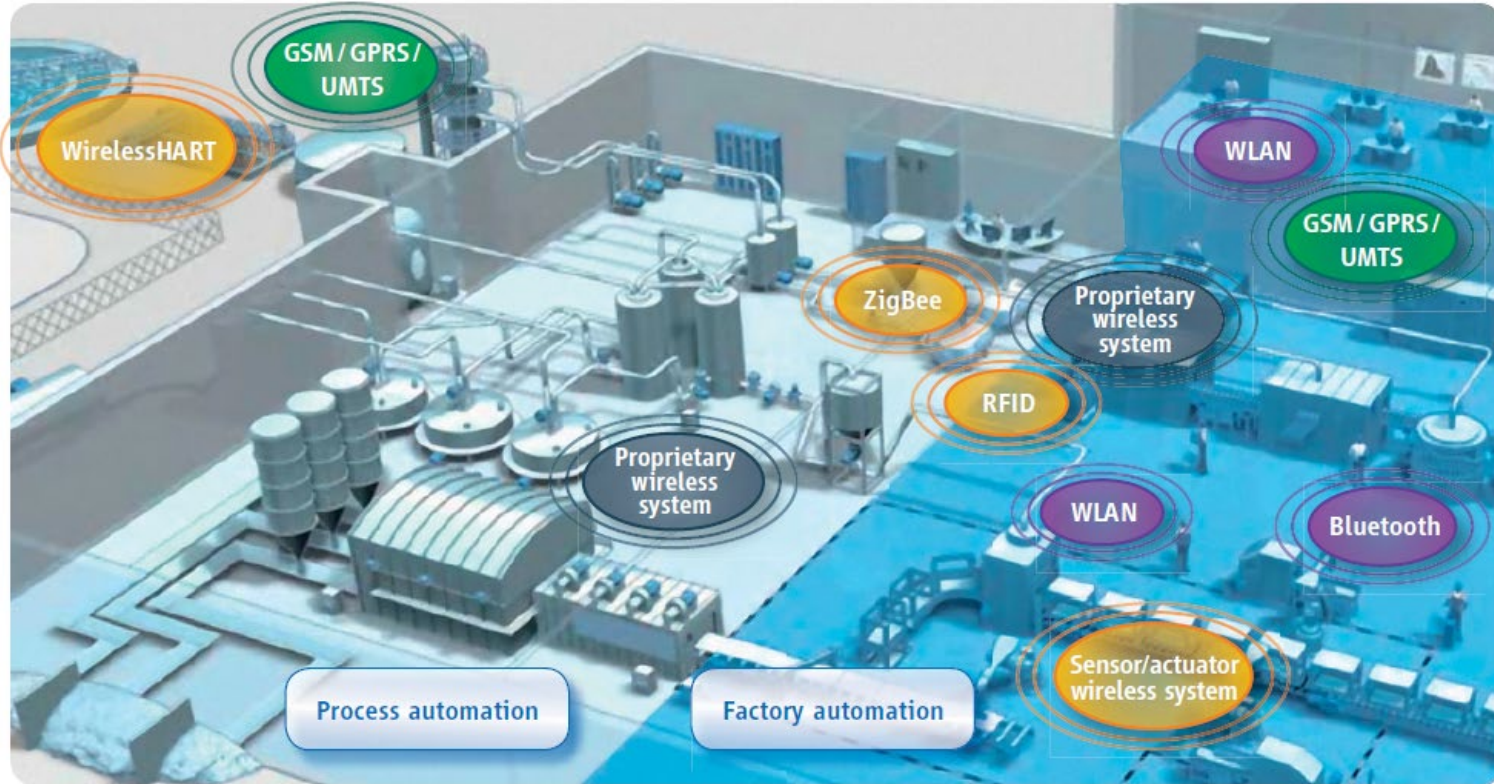
Industrial WLAN: Besonderheiten drahtloser Kommunikation

- dynamisch veränderbare Entfernung
- dynamische veränderbare Qualität
- dynamisch veränderbare Anzahl von Stationen

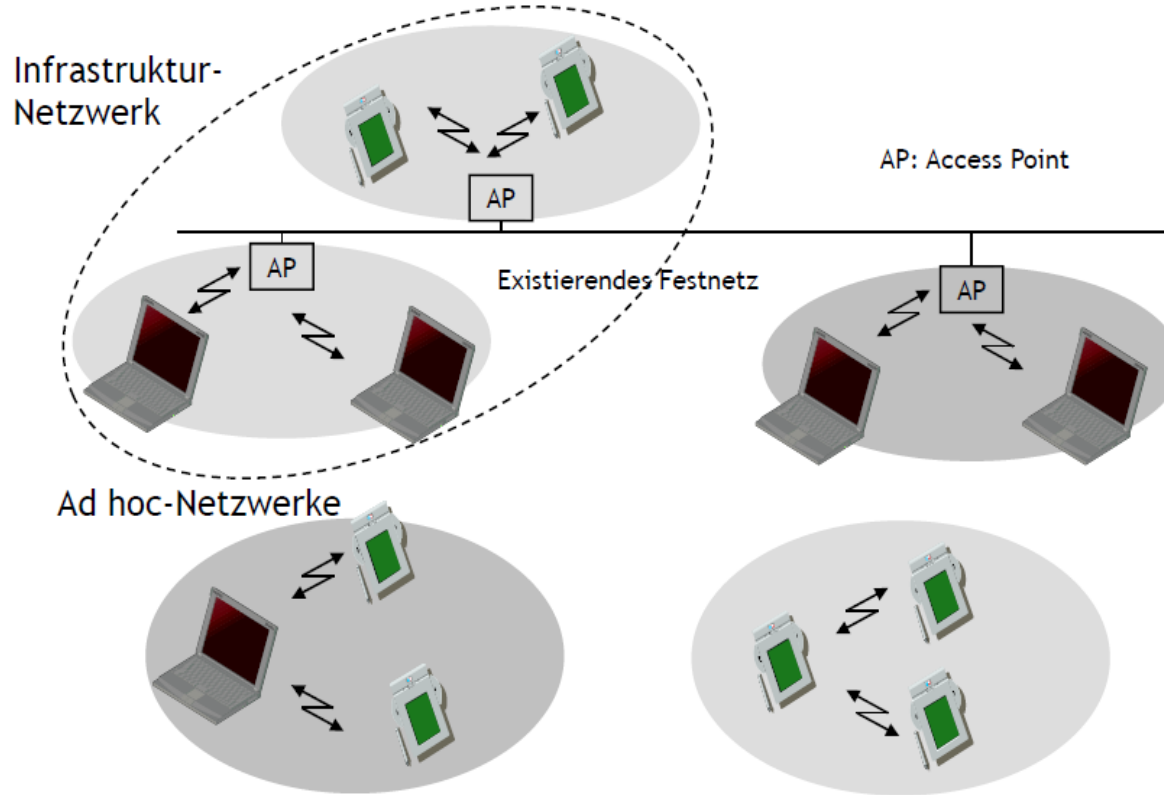
Industrial WLAN: Anwendungen drahtloser Kommunikation



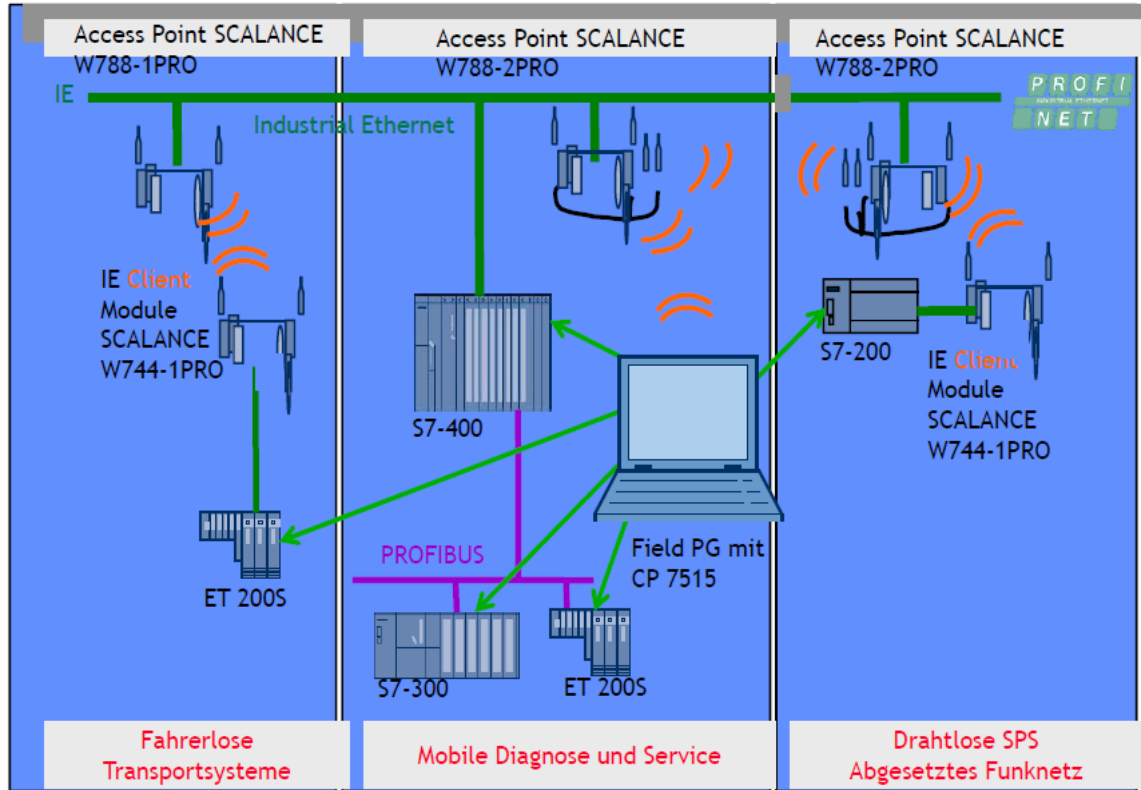
Industrial WLAN: Anwendungen drahtloser Kommunikation



Industrial WLAN: Vergleich Infrastruktur und Ad-Hoc Netzwerke



Industrial WLAN: Einsatz am Beispiel Profinet

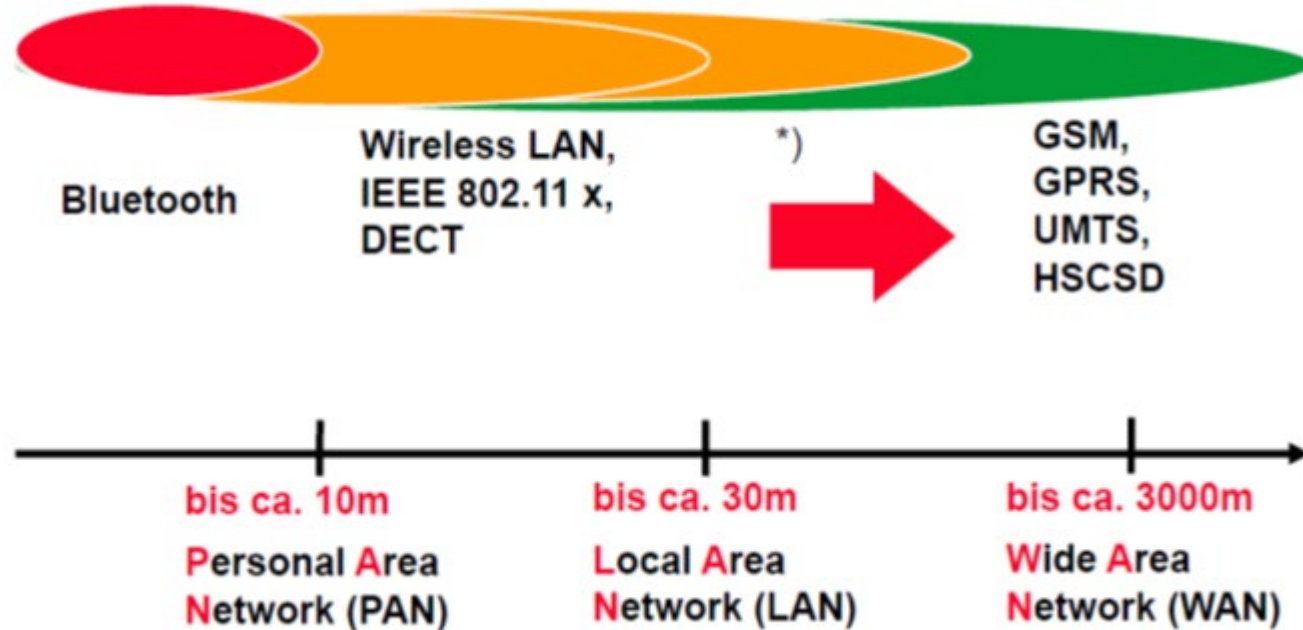


Industrial WLAN: WLAN Accesspoint und Netzübergangstation

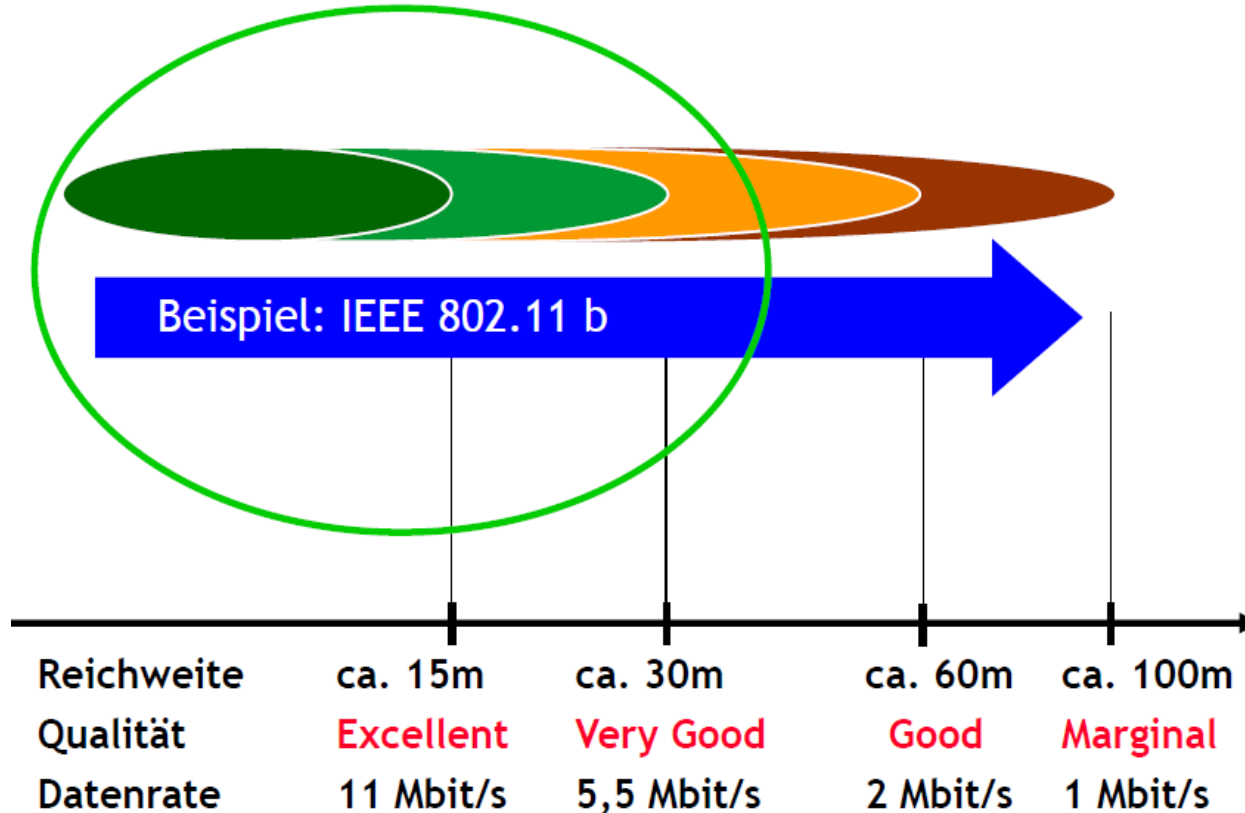


Industrial WLAN: Reichweite von Wireless-Netzwerken

Standardisierte und verfügbare Funktechnik



Industrial WLAN: Übertragungsqualität vs. Reichweite (indoor)



Industrial WLAN: Reichweiten

➤ Übertragungsbereich

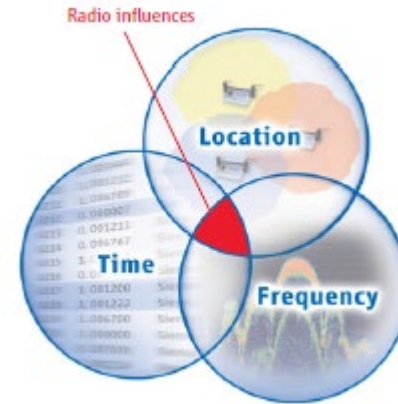
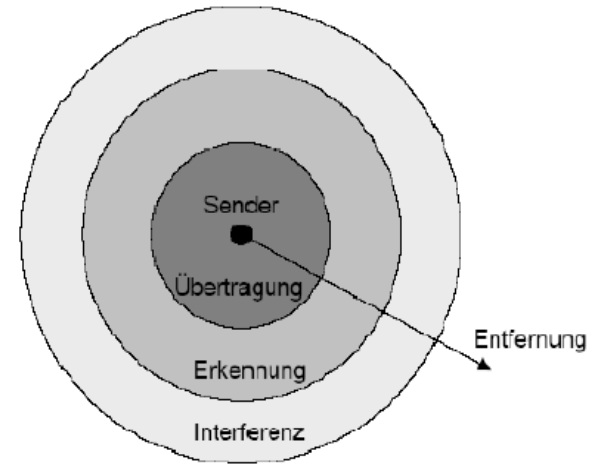
- Kommunikation möglich
- niedrige Fehlerrate

➤ Erkennungsbereich

- Signalerkennung möglich
- Keine Kommunikation möglich

➤ Interferenzbereich

- Signal kann nicht detektiert werden
- Signal trägt zum Hintergrundrauschen bei



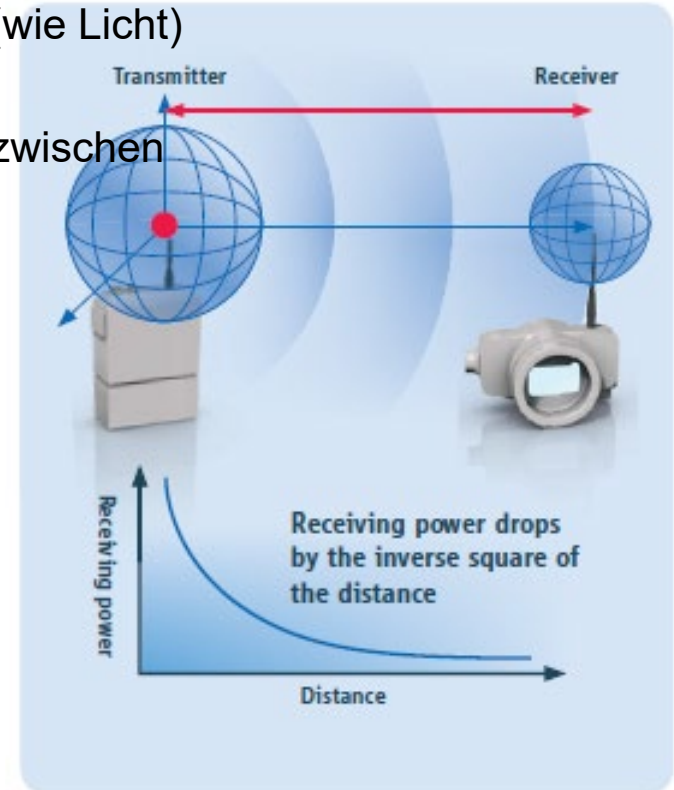
Industrial WLAN: Dämpfung/Verzerrung

➤ Ausbreitung im freien Raum grundsätzlich geradlinig (wie Licht)

➤ Empfangsleistung nimmt mit $1/d^2$ ab (d = Entfernung zwischen Sender und Empfänger)

➤ Empfangsleistung wird u.a. beeinflusst durch

- Freiraumdämpfung (frequenzabhängig)
- Abschattung durch Hindernisse
- Reflektion an großen Flächen
- Streuung (scattering) an kleinen Hindernissen
- Beugung (diffraction) an scharfen Kanten



Industrial WLAN: Medienzugriffsverfahren

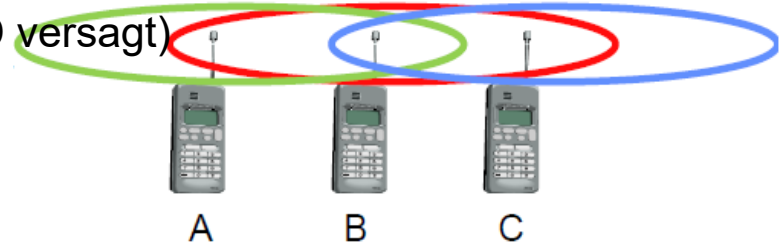
- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection)
 - Senden, sobald das Medium frei ist, hören, ob eine Kollision stattfand (ursprüngliches Verfahren im Ethernet IEEE802.3)

- **Probleme in drahtlosen Netzen**
 - Signalstärke nimmt quadratisch mit der Entfernung ab
 - CS und CD werden beim Sender eingesetzt, aber Kollision geschieht beim Empfänger
 - Kollision ist dadurch unter Umständen nicht mehr beim Sender hörbar, d.h. CD versagt
 - weiterhin kann auch CS falsche Ergebnisse liefern, z.B. wenn ein Endgerät „versteckt“ ist

Industrial WLAN: Versteckte Endgeräte

➤ „Verstecktes“ Endgerät

- A sendet zu B, C empfängt A nicht mehr
- C will zu B senden, Medium ist für C frei (CS versagt)
- Kollision bei B, A sieht dies nicht (CD versagt)
- A ist „versteckt“ für C



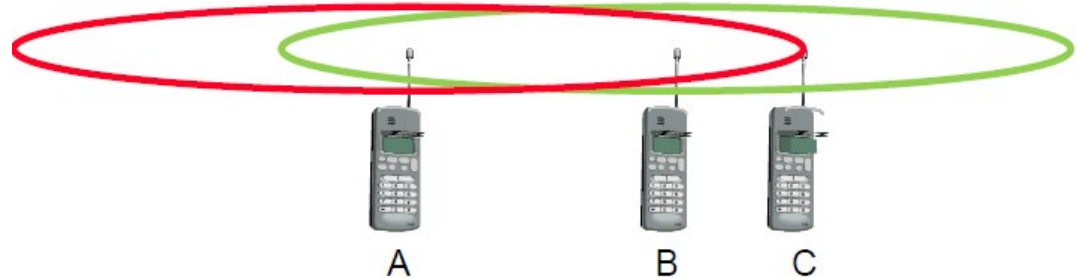
➤ „Ausgeliefertes“ Endgerät

- B sendet zu A, C will zu einem Gerät senden (nicht A oder B)
- C muss warten, da CS ein „besetztes“ Medium signalisiert
- da A aber außerhalb der Reichweite von C ist, ist dies unnötig
- C ist B „ausgeliefert“

Industrial WLAN: Nahe und ferne Endgeräte

➤ Endgeräte A und B senden, C soll empfangen

- die Signalstärke nimmt quadratisch mit der Entfernung ab
- daher „übertönt“ das Signal von Gerät B das von Gerät A
- C kann A nicht hören



Industrial WLAN: Übertragungsverfahren

- **Basisband** (bitserielle Übertragung oder Bitübertragung)
 - Digitales Übertragungsverfahren
 - Digitale Information wird als Folge von Bits unmoduliert, rechteckförmig übertragen.
- **Trägerband** (binäre Modulation oder Umtastung)
 - Analoges Übertragungsverfahren.
 - Digitale Information wird auf Trägerfrequenz aufmoduliert.
- **Breitband** (broadband)
 - Analoges Übertragungsverfahren (Ursprung: Kabel-Fernsehtechnik)
 - Gestattet die Übertragung vieler Kanäle auf einem Übertragungsmedium (Video, Daten, Sprache).
 - Sende- und Empfangskanal werden getrennt übertragen.

Industrial WLAN: Signalbildung & Modulation

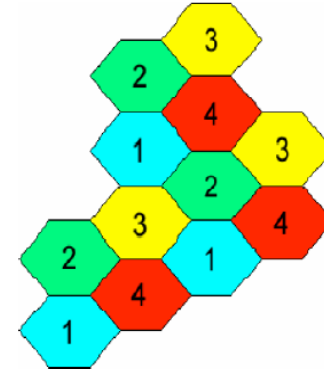
- **Ziel:** Möglichst viele Datenbits pro Zeit übertragen
- Übertragungskanal hat eingeschränkte Bandbreite => im allgemeinen keine (ideale) Basisbandübertragung (Digitale Rechteckverläufe) möglich
- **Modulation:**
 - Bandbeschränkte Kanäle, Mehrfachausnutzung
 - Änderung von charakteristischen Merkmalen einer Trägerfrequenz
 - Änderung proportional zum Steuersignal
 - Empfänger misst die Merkmale und konstruiert daraus das Steuersignal

Industrial WLAN: Multiplexing und Wireless

- Ziel ist Mehrfachnutzung des gemeinsamen Mediums.
- Multiplexen ist in 4 Dimensionen möglich.

Industrial WLAN: SDMA

- **SDMA** (Space Division Multiple Access)
 - im Raum (ri)
 - Einteilung des Raums in Sektoren, gerichtete Antennen
 - Wird in allen zellularen Netzen eingesetzt
 - Wiederverwendung von Frequenzen in entfernten Zellen
 - Zelle enthält eine Menge von Frequenzbändern so zugeordnet, dass es keine gleichen Frequenzen mit Nachbarzellen gibt
 - 4-Zellen-Wiederholungsmuster:



Industrial WLAN: TDMA

➤ TDMA (Time Division Multiple Access)

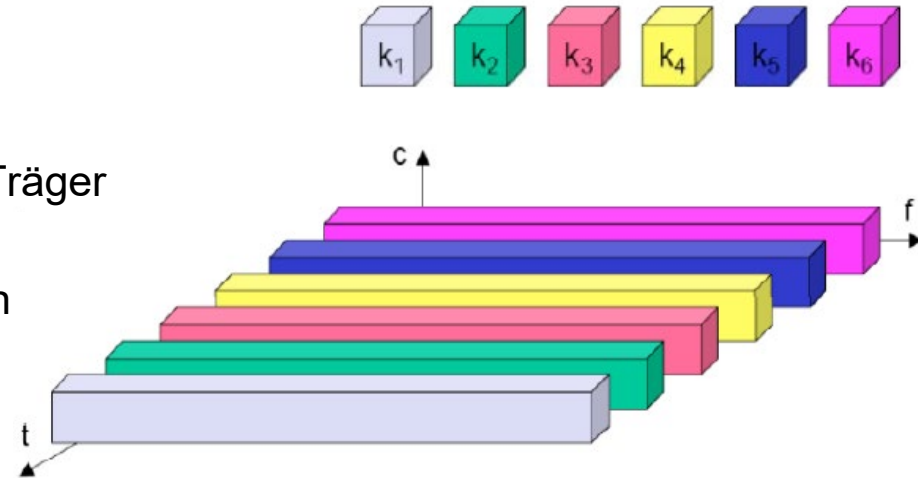
- Im Zeitbereich (t)
- Zeitlich gesteuertes Zugriffsrecht eines Übertragungskanals
- Kanal belegt den gesamten Frequenzraum für eine Zeitabschnitt

▪ Vorteile

- In einem Zeitabschnitt nur ein Träger auf dem Medium
- Durchsatz bleibt auch bei vielen Teilnehmern hoch

▪ Nachteile

- Genaue Synchronisation nötig



Industrial WLAN: FDMA

➤ **FDMA** (Frequency Division Multiple Access)

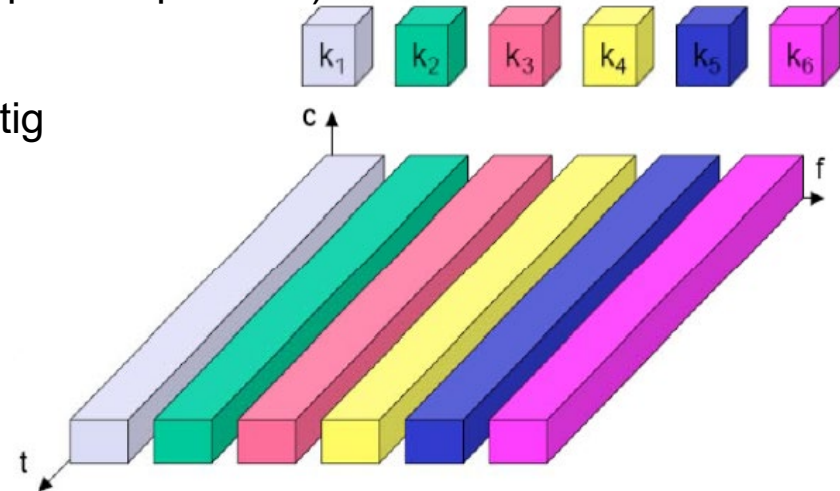
- Im Frequenzbereich (f)
- Zuordnung eines Übertragungskanal zu einer Frequenz
- Kanal belegt Frequenzabschnitt über gesamten Zeitraum
- Permanent (z.B. Rundfunk), in Verbindung mit TDMA (z.B. GSM), schnelles Springen (FHSS, Frequency Hopping Spread Spectrum)

▪ **Vorteile**

- Keine dynamische Koordination nötig
- Auch für analoge Signale

▪ **Nachteile**

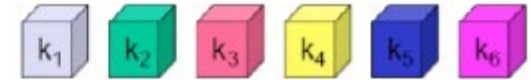
- Bandbreitenverschwendung bei ungleichmäßiger Belastung
- Unflexibel



Industrial WLAN: TDMA und FDMA

➤ TDMA & FDMA

- Kombination der oben genannten Verfahren (t und f)
- Sendungen belegen Frequenzabschnitt für einen Zeitabschnitt
- Beispiel: GSM

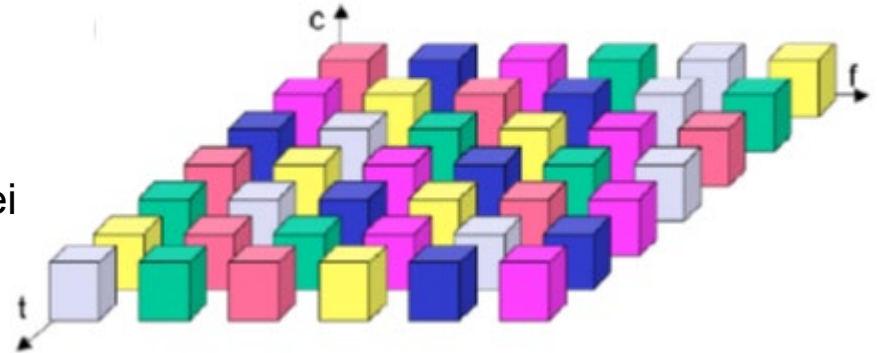


▪ Vorteile

- Relativ abhörsicher
- Schutz gegen Störungen
- Höhere Benutzerdatenrate als bei Codemultiplex möglich

▪ Nachteile

- Genaue Koordination erforderlich



Industrial WLAN: CDMA

➤ **CDMA** (Code Division Multiple Access)

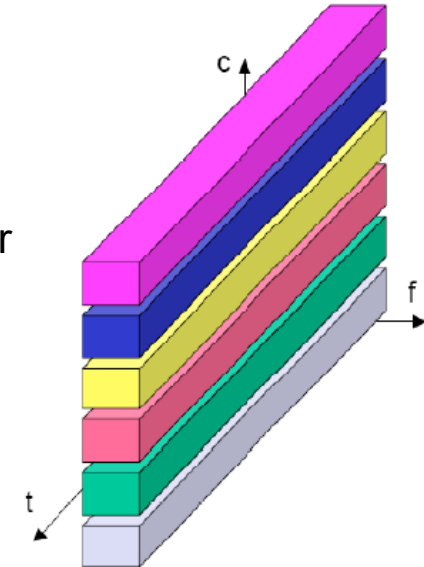
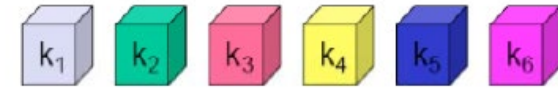
- In einem Coderaum (c)
- Alle Stationen operieren zur gleichen Zeit auf der gleichen Frequenz
- XOR-Verknüpfung mit „Code“

▪ **Vorteile**

- Keine Frequenzplanung
- Sehr großer Coderaum im Vergleich zum Frequenzraum
- Störungen nicht codiert
- Vorwärtskorrektur und Verschlüsselung leicht integrierbar

▪ **Nachteile**

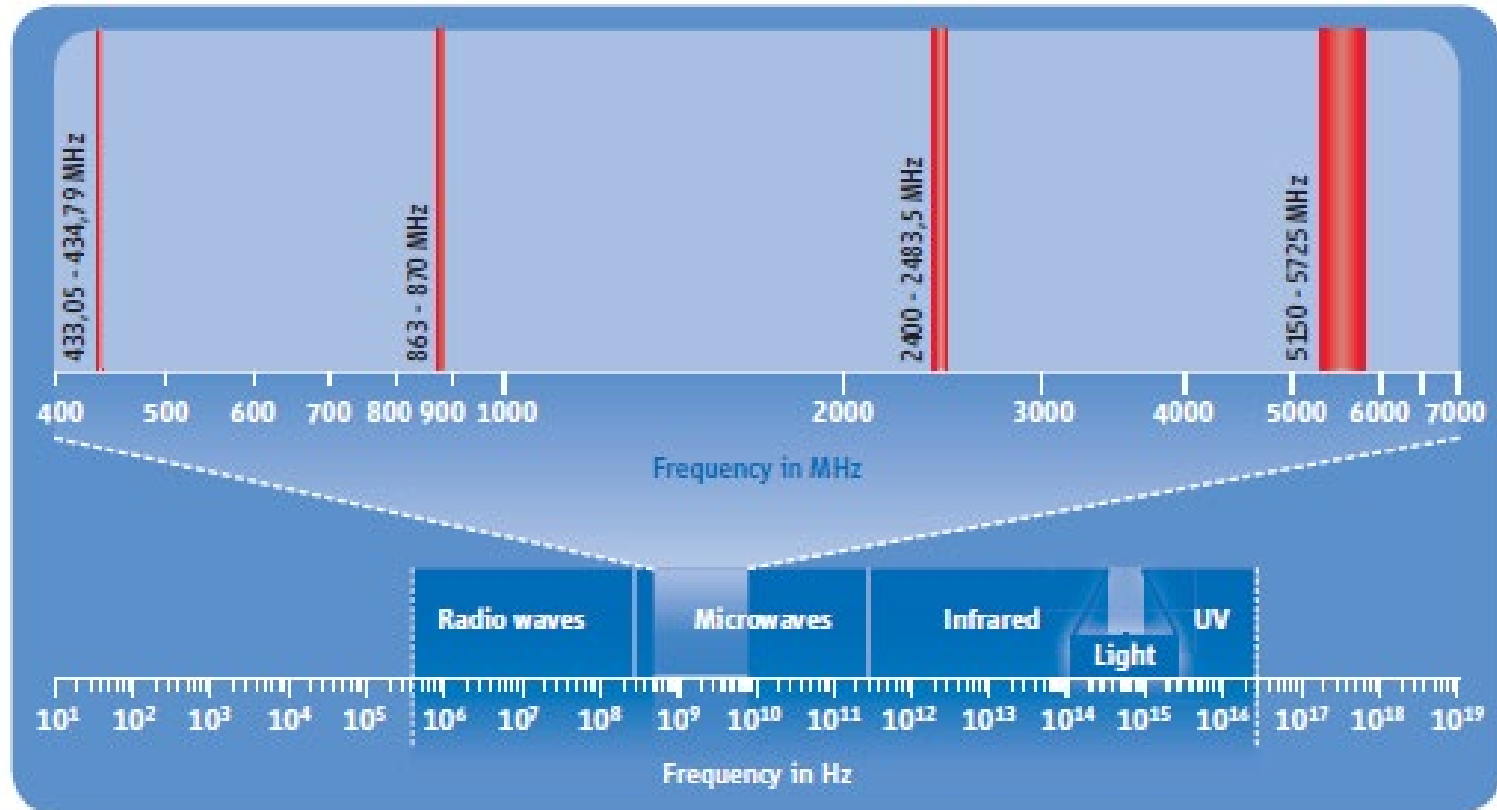
- Höhere Komplexität wg. Signalgenerierung
- Alle Signale müssen beim Empfänger gleich stark sein



Industrial WLAN: Vergleich Multiplexing

Verfahren	SDMA	TDMA	FDMA	CDMA
Idee	Einteilung des Raums in Zellen/Sektoren	Aufteilen der Sendezeiten in disjunkte Schlitze, anforderungs-gesteuert oder fest	Einteilung des Frequenzbereichs in disjunkte Bänder	Bandspreizen durch individuelle Codes
Teilnehmer	nur ein Teilnehmer kann in einem Sektor ununterbrochen aktiv sein	Teilnehmer sind nacheinander für kurze Zeit aktiv	jeder Teilnehmer hat sein Frequenzband, ununterbrochen	alle Teilnehmer können gleichzeitig am gleichen Ort ununterbrochen aktiv sein
Signal-trennung	Zellenstruktur, Richtantennen	im Zeitbereich durch Synchronisation	im Frequenzbereich durch Filter	Code plus spezielle Empfänger
Vorteile	sehr einfach hinsichtlich Planung, Technik, Kapazitätserhöhung	etabliert, voll digital, vielfältig einsetzbar	einfach, etabliert, robust, planbar	flexibel, benötigt weniger Frequenzplanung, weicher handover
Nachteile	unflexibel, da meist baulich festgelegt	Schutzzeiten wegen Mehrwegausbreitung nötig, Synchronisation	geringe Flexibilität, Frequenzen Mangelware	komplexe Empfänger, benötigt exakte Steuerung der Sendeleistung
Bemerkung	nur in Kombination mit TDMA, FDMA oder CDMA sinnvoll	Standard in Festnetzen, im Mobilien oft kombiniert mit FDMA	heute kombiniert mit TDMA in z.B. GSM	Findet Verwendung in UMTS

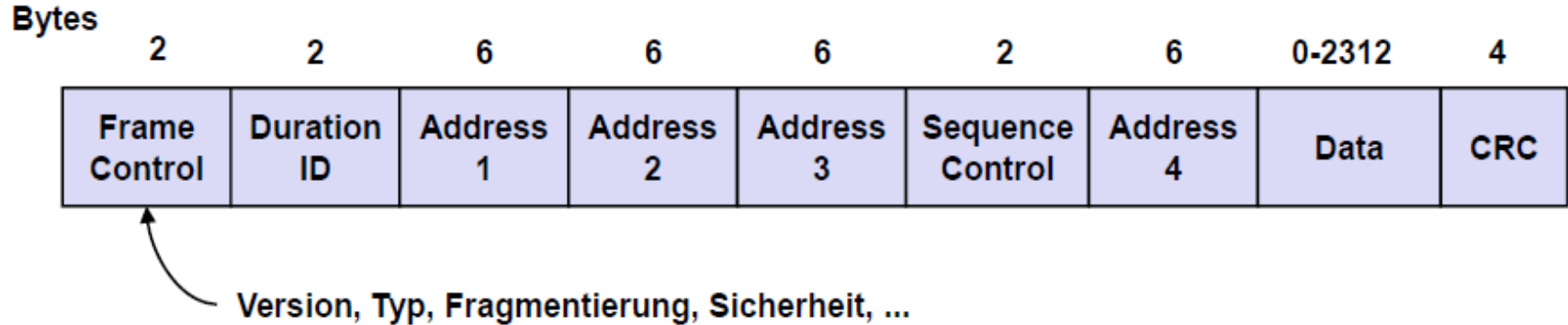
Industrial WLAN: Frequenzbereiche für Datenkommunikation



Industrial WLAN: Übersicht WLAN (IEEE 802.11)

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frequenzbereich	5.150-5.350 MHz 5.725-5.825 MHz	2.400-2.4835 MHz	2.400-2.4835 MHz
Bitrate	54 Mbit/s	11 Mbit/s	54 Mbit/s
Anzahl Kanäle (nicht-überlappend)	bis zu 12	3	3
Medium Access	CSMA/CA	CSMA/CA	CSMA/CA
Maximale Reichweite -LOS -NLOS	30...350m (54...6 Mbit/s) 18...90m (54...6 Mbit/s)	150...450m (11...1 Mbit/s) 30...90m (11...1 Mbit/s)	75...400m (54...1 Mbit/s) 25...90m (54...1 Mbit/s)
Kompatibilität	Nicht kompatibel zu IEEE 802.11 b/g	Marktführer, größte Verbreitung	Backward-kompatibel & Interoperabel mit 802.11b

Industrial WLAN: IEEE-Standard 802.11 Rahmenformat



Bluetooth: Idee

- Namensgebung geht auf **dänischen König Blauzahn** zurück
- Universelles Funksystem für drahtlose **Ad-hoc** Verbindungen
- Ad-hoc-Verknüpfung von Computer mit Peripherie, tragbaren Geräten, PDAs, Handys
- Eingebettet in viele Geräte
- Kleine **Reichweite (10-100 m), niedrige Leistungsaufnahme, lizenzfrei im 2,45 GHz-ISM-Band**
- Sprach- und Datenübertragung mit ca. **1 Mbit/s** Bruttodatenrate
- Idee: **kleine, spontane Netzwerke mit relativ hoher Datenübertragungsrate**

Bluetooth: Special Interest Group

- **Gründungsmitglieder:** Ericsson, Intel, IBM, Nokia, Toshiba
- Später hinzugekommene Förderer: 3Com, Agere (früher: Lucent), Microsoft, Motorola
- **über 2500 Mitglieder**
- Gemeinsame Spezifikation und Zertifizierung von Produkten

Bluetooth: Merkmale

- 2,4 GHz ISM Band, 79 Kanäle, 1 MHz Trägerabstand
 - Kanal 0: 2402 MHz ... Kanal 78: 2480 MHz
 - FSK Modulation, 1-100 mW Sendeleistung
- **FHSS** (Frequency Hopping Spread Spectrum) und **TDD** (Time Division Duplex)
 - Frequenzsprungverfahren (FHSS) mit 1600 Sprüngen/s (→ Robustheit gegenüber Störungen)
 - Sprungfolge pseudozufällig, vorgegeben durch einen Master
 - TDD zur Richtungstrennung: Hierbei wird das Sende- und Empfangssignal im gleichen Frequenzband zu unterschiedlichen Zeiten nacheinander übertragen (→ Aufteilung in Zeitschlitz).
- **Sprachverbindung - SCO** (Synchronous Connection Oriented)
 - FEC (forward error correction)→ redundante Kodierung, keine Übertragungswiederholung, 64 kbit/s duplex, Punkt-zu-Punkt, leitungsvermittelt

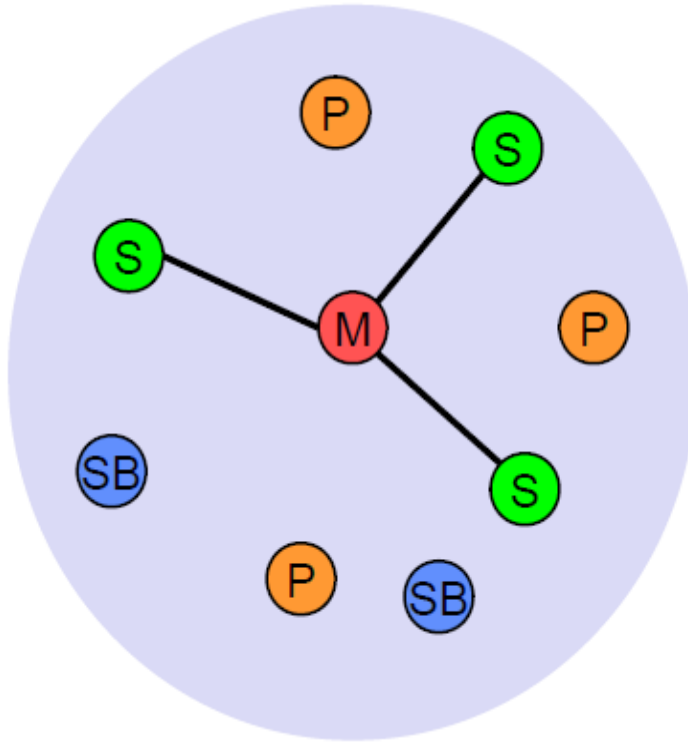
Bluetooth: Merkmale

- **Datenverbindung – ACL** (Asynchronous ConnectionLess)
 - asynchron, schnelle Bestätigung, Punkt-zu-Mehrpunkt, bis zu 433,9 kbit/s symmetrisch oder 723,2/57,6 kbit/s asymmetrisch, paketvermittelt
- **Topologie**
 - Überlappende Piconetze (Sterne) bilden ein „Scatternet“ (Streunetz)
- **Sicherheit**
 - Authentifizierung und Verschlüsselung (optional)

Bluetooth: Piconetze

- Eine Ansammlung von Geräten welche spontan (ad-hoc) vernetzt wird
- Ein Gerät wird zum Master, die anderen verhalten sich als Slaves während der Lebensdauer des Piconetzes
- Der Master bestimmt die Sprungfolge, die Slaves müssen sich darauf synchronisieren
- Jedes Piconetz hat eine eindeutige Sprungfolge
- Teilnahme an einem Piconetz = Synchronisation auf die Sprungfolge
- Jedes Piconetz hat einen Master und gleichzeitig bis zu 7 Slaves (>200 können „geparkt“ werden)

Bluetooth: Piconetze



M=Master
S=Slave
P=Parked
SB=Standby

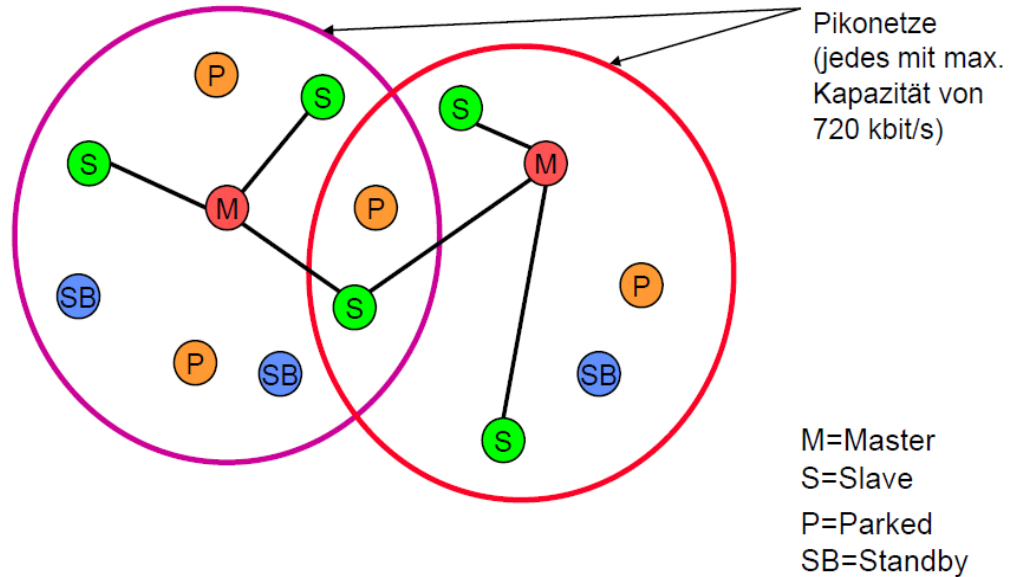
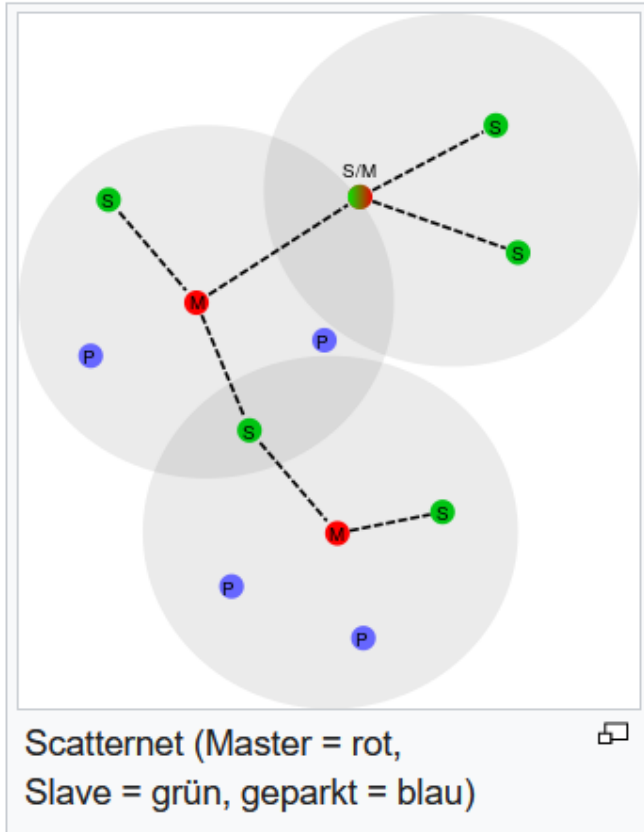
Bluetooth: Bildung eines Piconetzes

- Alle Geräte im Piconetz springen synchron
 - Der Master übergibt den Slaves seine Uhrzeit und Geräteerkennung
 - Sprungfolge: bestimmt durch die Geräteerkennung (48 bit, weltweit eindeutig)
 - Die Phase in der Sprungfolge wird durch die Uhrzeit bestimmt
- Adressierung
 - Active Member Address (AMA, 3 bit)
 - Parked Member Address (PMA, 8 bit)

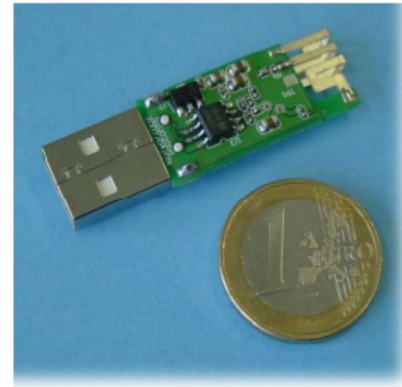
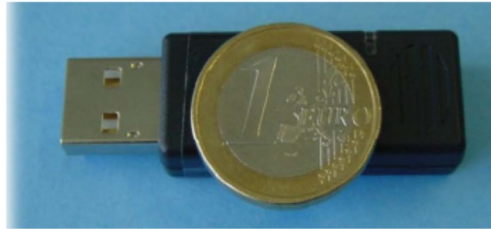
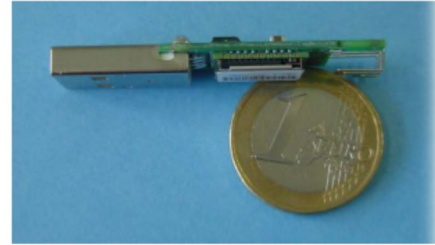
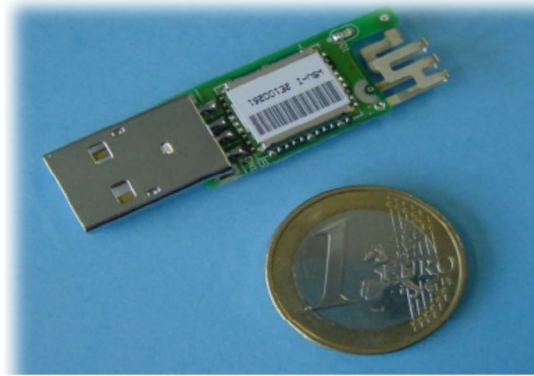
Bluetooth: Scatternetz

- Verbindung mehrerer räumlich naher Piconetze durch gemeinsame Master- oder Slave-Geräte
 - Geräte können Slaves in einem Piconetz sein, Master in einem anderen Piconetz
- Kommunikation zwischen Piconetzen
 - Geräte, welche zwischen den Piconetzen hin und her springen

Bluetooth: Scatternetz



Bluetooth: Beispiele Bluetooth/USB-Adapter



Bluetooth: Beispiel Industrial Bluetooth



Zigbee: Was ist das?

- Ein Industriestandard für Funknetze
- Entwickelt von der **Zigbee-Alliance** (aktuell ca. 230 Unternehmen, darunter Mitsubishi, Philips und Samsung)
- Namensgebend ist der Tanz der Honigbienen
- Speziell für energiesparende, kabellos kommunizierende Endgeräte mit geringen Datenraten konzipiert (technologisch einfacher und preiswerter als Bluetooth)
- Zigbee Standard baut auf dem **IEEE 802.15.4 Standard** auf
- Anwendungen: vor allem Heim- und Gebäudeautomatisierung, aber auch Industrie- und Automatisierungstechnik, WSN und Medizintechnik

Zigbee: Beispiel Hausautomation



Schalter



Steckdose
Osram Lightify Plug



Raspi Adapter

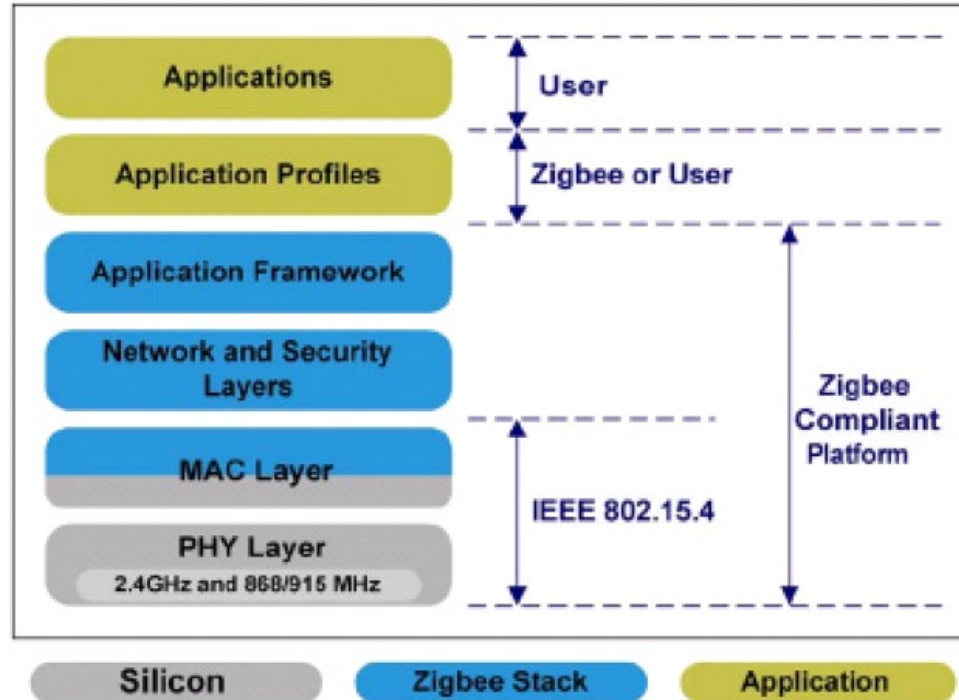


Osram Smart+
Lampe mit ZigBee



Xbee Adapter
Mit AT Befehlen

Zigbee: IEEE 802.15.4 Standard



<http://www.eetimes.com/showArticle.jhtml?articleID=173600329>

Zigbee: Technologie

- Die Datenraten bei Zigbee liegen bei **20kbit/s, 40kbit/s und 250kbit/s**. Dies hängt mit den in Europa und USA benutzten ISM Bändern zusammen.
- ISM (Industrial, Scientific, Medical): lizenzfreie Frequenzbänder für ISM-Anwendungen
- In **Europa**: ISM-Band um **868 MHz**, Datenrate von **20kbit/s**.
- In den **USA**: ISM-Band um **916 MHz**, 10 Kanäle mit **40kbit/s** Datenübertragungsrate
- ISM-Band von **2,4 GHz**: 16 Kanäle mit einer Datenübertragungsrate von **250kbit/s**
- Die **Reichweite** der Datenübertragung liegt je nach Sendeleistung **zwischen 10 und 75 Metern**.

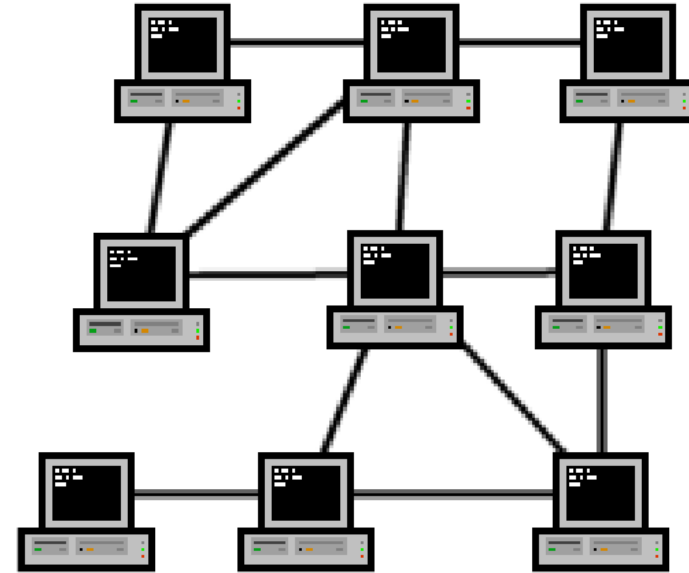
Quelle: https://wwwvs.cs.hs-rm.de/vs-wiki/images/9/9e/SeminarausarbeitungThossBeckmann_SS2014_Armin_KarasalihovicFinal.pdf

Zigbee: Technologie

Das Zigbee Protokoll unterstützt mehrere Arten von Netzwerktopologien, wie z.B.:

- Point-to-Point
- Point-to-Multipoint
- Mesh

In einem Mesh-Netzwerk sind Geräte mit anderen Geräten in mehreren Pfaden verbunden. Die Pfade werden dynamisch optimiert und angepasst, d.h. ein Gerät merkt, wenn ein anderes wegfällt oder hinzukommt und kann so entsprechend sein Routing anpassen.



Quelle: https://wwwvs.cs.hs-rm.de/vs-wiki/images/9/9e/SeminararbeitThossBeckmann_SS2014_Armin_KarasalihovicFinal.pdf

Zigbee: Technologie

Es gibt 3 gerätearten, welche in einem ZigBee Netzwerk zu finden sind:

- Coordinator
- FFD – Full Functional Device
- RFD – Reduced Functional Device

Coordinator: verwaltet das ZigBee Netzwerk und existiert nur einmal im Netzwerk. Bei ihm können sich Geräte an- bzw. Abmelden. Der Coordinator gibt die Parameter des Netzwerks vor.

FFD: kann Daten von anderen Geräten weiterleiten und sich an einem Netzwerk anmelden.

RFD: kann keine Daten weiterleiten. Es kann Befehle vom Netzwerk erhalten und seinen Status wiedergeben.

Zigbee: Technologie

Zur Erhöhung der Zuverlässigkeit arbeitet das ZigBee-Protokoll nach dem **Handshake-Prinzip** und das Zugriffsverfahren für die Kanäle ist **CSMA/CA**.

Handshake-Prinzip: Empfänger bestätigen den Empfang von Daten und teilen mit, dass sie weitere Daten empfangen können.

Wiederholung CSMA/CA: Regelt den Vielfachzugriff und die Kollisionsvermeidung. Die Geräte horchen das Übertragungsmedium für eine Zeit ab, senden dann ein Ready-to-Send auf das Medium. Danach erhalten sie ein Clear-to-Send und senden folglich ihre Daten. Das Ende der Übertragung wird mit einem Acknowledgment angezeigt.

Die **Modulation** bei ZigBee ist **PSK** (Phase Shift Keying).

Quelle: https://wwwvs.cs.hs-rm.de/vs-wiki/images/9/9e/SeminarausarbeitungThossBeckmann_SS2014_Armin_KarasalihovicFinal.pdf

Zigbee im Vergleich...

Protokoll	ZigBee	EnOcean	Z-Wave	NFC	HomeMatic	Dash7	KNX	Bluetooth	WLAN
Frequenz (MHz)	868 / 915 / 2400	868	868	13,56	868	433	868	2400	2400
Frequenzbelastung	G / G / Hoch	Gering	Gering	Extrem Gering	Gering	Sehr gering	Gering	Hoch	Hoch
Kollisionsrisiko	Mittel	Sehr gering	Mittel	Sehr gering	Mittel	Gering	Mittel	Sehr gering	Hoch
Datenrate (kbit/s)	20 / 40 / 250	125	9,6	424	n/a	200	16	720	10k ++
Energiebedarf	Gering	Extrem gering	Gering	Gering	n/a	Gering	Gering	Mittel	Hoch
Reichweite (m)	10 – 75	30 – 300	30 – 200	0,1	10 – 100	Bis 1000	30 – 300	Bis 100	Bis 100
Batterielos?	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein
Modulation	PSK	ASK	FSK	ASK	FSK	FSK	FSK	PSK	PSK
Netzwerkgröße	64k	2 ³²	232	2	n/a	2 ³²	10k+	2 ¹⁶	2 ³²

Tabelle 1 Vergleich drahtloser Kommunikationslösungen

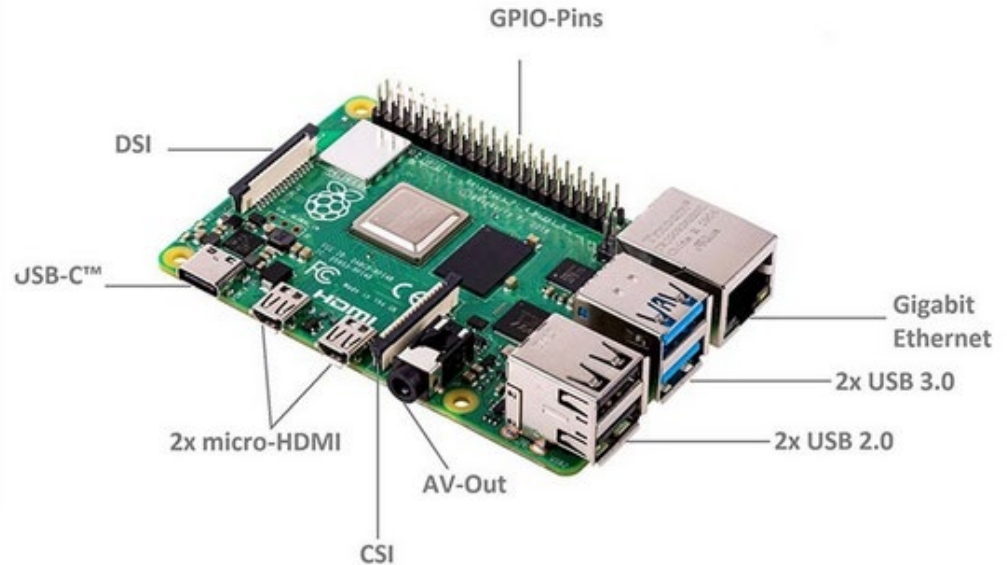
Quelle: https://www.vvcs.hs-rm.de/vs-wiki/images/9/9e/SeminausarbeitungThossBeckmann_SS2014_Armin_KarasalihovicFinal.pdf

Ausblick

Arduiono



Raspberry Pi



UbiComp – Teil 9: Industrial WLAN, Bluetooth & Zigbee

Fragen?

Prof. Dr.-Ing. Dorothea Schwung